PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-215452

(43)Date of publication of application : 06.08.1999

(51)Int.Cl. H04N 5/765
H04N 5/781

(21)Application number : 10-011408

(22)Date of filing : 23.01.1998

(71)Applicant : SEIKO EPSON CORP

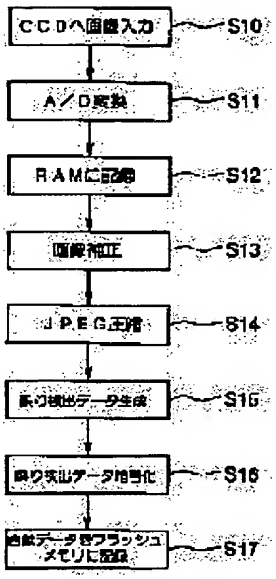
(72)Inventor : NAKAJIMA YASUMASA
ICHIHARA SHINTARO
MOGAMI KAZUTO

(54) DIGITAL CAMERA AND IMAGE AUTHENTICATION SYSTEM USING THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To allow a system to confirm whether or not image data have been altered from image data at photographing.

SOLUTION: An electric signal outputted from a CCD is converted into a digital signal in a step S11. Digital data outputted from an A/D converter are stored in a RAM in a step S12. Various image corrections are applied to the data stored in the RAM in a step S13. The data corrected in the step S13 are compressed by the JPEG system in a step S14. Error detection data are generated from the compressed image data in a step S15. Error detection data are encrypted in a step S16 to obtain encrypted data. The image data and the encrypted data are stored in a flash memory as a JPEG file, in cross reference with each other in a step S17.



LEGAL STATUS

[Date of request for examination] 09.09.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3521723

[Date of registration] 20.02.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] The digital camera characterized by having a means to associate and output the photosensor which has two or more pixels, a means to change the output of said photosensor into the image data which consists of a digital signal, the record medium which records said image data, a means to generate error detection data from said image data, and said image data and said error detection data.
[Claim 2] The digital camera according to claim 1 characterized by having a means to encipher said error detection data.
[Claim 3] Said record medium is a digital camera according to claim 1 or 2 characterized by being able to detach and attach freely, and for said image data and said error detection data relating, and recording them.
[Claim 4] The image authentication system which is an image authentication system using a digital camera given in any 1 term of claims 1-3, and is characterized by having a means to input image data and error detection data, and a means to collate said image data with said error detection data.

[Translation done.]

* NOTICES *
JPO and NCIPI are not responsible for any
damages caused by the use of this translation.
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the digital camera which records the photoed image as digital data.
[0002]
[Description of the Prior Art] Conventionally, when taking a photograph, the light incorporated from the lens is irradiated on a film, and the camera with which an image is recorded because a chemical reaction occurs is used. With the above-mentioned camera, a film can be developed and a photograph can be printed by the ability being burned on printing paper. Since the reaction of a silver chloride is generally used as the above-mentioned chemical reaction, the photograph taken with such a camera is called film

photo.
[0003] On the other hand, in recent years, after changing light into an electrical signal with photosensors, such as CCD, and changing it into a digital signal, the digital camera recorded on record media, such as a flash memory, has spread. If a digital camera is used, preservation and various processings of an image can be individually performed easily using a personal computer etc., and also a photograph can be printed, without developing a film by outputting by the printer. By improvement in the printing quality of a printer, the high photograph of quality can also be printed, so that distinction hardly sticks with a film photo.
[0004]
[Problem(s) to be Solved by the Invention] However, since it can be processed without being able to process easily the image photoed with the digital camera with a personal computer etc., and leaving the marks of processing as compared with a film photo when it is going to use the photograph taken with the digital camera for certification photographs, such as property damage insurance, it is difficult to distinguish, even if the altered so-called photograph which was processed unjustly is used, and there is a problem that there is a possibility that it may be abused.
[0005] Therefore, the purpose of this invention is to offer the image authentication system using the digital camera and it which output the image data which can check whether it has been changed from the image data at the time of photography.
[0006]
[Means for Solving the Problem] According to the digital camera of this invention according to claim 1, it has a means to associate and output a means to generate error detection data, and image data and error detection data, from the image recording medium which records image data, and image data. Therefore, since image data and error detection data serve as mismatching when at least 1 bit of image data recorded on the record medium at the time of photography is changed after an output from a digital camera, it can be judged that image data was changed after photography. Moreover, if the adjustment of image data and error detection data can be taken, it can be judged that an image is still in the state at the time of photography. As an approach of generating error detection data, the approach of asking for the checksum of image data, CRC (Cyclic Redundancy check) or an one-way hash function (one-way hash function), etc. can be used.
[0007] According to the digital camera of this invention according to claim 2, since it is enciphered, it can be changed into another image data from which image data can obtain the same error detection data, and error detection data can prevent rewriting error detection data to compensate for modification of image data.
[0008] According to the digital camera of this invention according to claim 3, since an image recording medium can be detached and attached freely, it can use an image recording medium as an output means from a digital camera. Moreover, when reading the image recording medium removed from a digital camera directly with a personal computer etc. and inputting image data, in order to output as image data which can judge whether it was changed from the time of photography, it is required for image data and error detection data to relate and to record them on an image recording medium.
[0009] Since it has a means to input image data and error detection data, and a means to collate image data with error detection data according to the image authentication system of this invention according to claim 4, it can judge whether it was changed after the inputted image data was recorded with the digital camera.
[0010]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail based on a drawing.
[0011] Drawing 2 is a block diagram for explaining the digital camera 1 of the example of this invention. It consists of interfaces 17 for outputting the contents of a control unit 11, a condenser lens 12, CCD (Charge CoupledDevice)13 as a photosensor, A/D converter 14, RAM (Random Access Memory)15, the

flash memory 16 as an image recording medium which records image data, and the flash memory 16 to external personal computer 20 grade etc. A control device 11 is equipped with CPU, ROM on which the program for performing various control of a digital camera 1 was recorded, and an I/O means.
[0012] Drawing 1 is a flow chart which shows the stroke to which photography is carried out with a digital camera 1. If a user pushes the shutter of a digital camera 1, at step S10, the light condensed with the condenser lens 12 will be inputted into CCD13, and will be changed into an electrical signal. The storage time of a diaphragm of a condenser lens 12 or shutter speed 13, i.e., CCD, is automatically controlled by the control unit 11 by directions of a user. As CCD13, a color picture can be photoed by using CCD13 by which two or more pixels which have the primary color filter of R (Red), G (Green), and B (Blue) as shown in drawing 3 R> 3 have been arranged in the shape of a matrix. CCD which has the complementary filter of C (Cyan), M (Magenta), Y (Yellow), and G (Green) may be used.
[0013] At step S11, the electrical signal outputted from CCD13 is changed into a digital signal by A/D converter 14, and in step S12, since the digital data outputted from A/D converter 14 is improvement in the speed, without minding a control unit 11 by DMA (Direct Memory Access), the address of direct RAM15 is specified and it is recorded. DRAM which has a self refresh function as RAM15 can be used.
[0014] At step S13, various kinds of image amendments, such as adjustment of a white balance, interpolation processing, and color correction, are performed about the data recorded on RAM15.
[0015] At step S14, in order to make [many] the record number of sheets to an image recording medium, the data amended at step S13 are compressed with methods, such as JPEG (Joint Photographic Experts Group), and image data with a small capacity is generated. JPEG can treat the image of about 16,700,000 colors of each color 256 gradation of R, G, and B, is the irreversible picture compression approach generally used, and can adjust preservation image quality by changing compressibility. A control unit 11 performs JPEG compression by software, and also the circuit of dedication can be used for improvement in the speed.
[0016] At step S15, a control device 11 generates error detection data based on the image data generated at step S14. As error detection data, a checksum can be used, for example. Here, what expressed image data 32 with the binary number presupposes that it is shown like drawing 4 . Since the total value and the checksum 33 which are called for from image data 32 will serve as mismatching when image data 32 is changed if total value without 8-bit carry of the longitudinal direction of image data is calculated in each line with a control device 11 and it is made into a checksum 33 as shown in A of drawing 4 , it can judge whether image data 32 was changed by collating image data 32 and a checksum 33. In this case, if 2 bits is changed in one line, the checksum 33 which calculated total value in each train also about 8 bits of a lengthwise direction as it was shown in B of drawing 4 , since having been changed was undetectable may be used further.
[0017] Moreover, a CRC method, an one-way hash function, etc. can apply how it is detectable whether the data other than a checksum are changed from original well-known about the error detection used for data communication etc. to this invention. By using these approaches, it can be said that it is very difficult to be able to assign different error detection data to each image data, and to reproduce the original image data from error detection data, and there is no practical problem.
[0018] At step S16, it enciphers with a control device 11 and considers as the encryption data 34 so that the error detection data of checksum 33 grade may not be analyzed or it may not be rewritten easily. Well-known approaches, such as a RAS method using a public key and a private key as the approach of encryption, can be used. The encryption data 34 enciphered with the private key are decipherable using the public key which became a private key and a pair. The private key is memorized in the digital camera 1, and must not be known by others. Moreover, a user does not need to know a private key. However, it is very difficult to ask for a private key from a public key. It can be changed into another image data from which image data 32 can obtain the same checksum 33 by this, and can prevent rewriting a checksum 33 to compensate for modification of image data 32.
[0019] At step S17, image data 32 and the encryption data 34 are recorded on the flash memory 16 as

an image recording medium as a JPEG file 30 at one. Even if it does not continue energizing a flash memory 16, it is the rewritable record medium which can hold the once recorded contents, is built in a digital camera 1, or is attached in the digital camera 1 free [attachment and detachment]. The JPEG file 30 consists of a header unit 31 which includes information, such as a data length and compressibility, as generally shown in drawing 5 , and image data 32. In the case of the JPEG file 30 recorded with a digital camera 1, information, such as photography conditions, such as a photography day and shutter speed, is also recordable on a header unit 31. In this example, the encryption data 34 are further added to a header unit 31, and are recorded on it.

[0020] It is able to be built in the digital camera 1, for the flash memory 16 to record the JPEG file 30 which does not contain the error detection data of encryption data 34 grade on the flash memory 16, when it cannot remove, and to generate error detection data in the phase outputted to the external personal computer 20 through an interface 17, and to add and output to the header unit 31 of the JPEG file 30. In addition, when distinguishing by the header unit 31 grade of the JPEG file 30 and transmitting to a personal computer 20 again, it is necessary to make it not add error detection data, when an image can be transmitted to a digital camera 1 from a personal computer 20.

[0021] On the other hand, a flash memory 16 can detach and attach freely from a digital camera 1, and when reading is possible, or when it has the function to correct an image to digital camera 1 the very thing, with the personal computer etc. in the contents, error detection data need to be recorded on coincidence in the phase where image data is recorded on a flash memory 16 in order to output image data and error detection data to one.

[0022] Moreover, although JPEG compression of the image data was carried out at step S14 at the degree of step S13, steps S15 and S16 were performed after that and generation and encryption of error detection data were performed in the flow chart of this example shown in drawing 1 , it is also possible to perform steps S15 and S16 to the degree of step S13, and to carry out JPEG compression of the image data at step S14 after it.

[0023] In order to judge whether the above digital cameras 1, the personal computer 20 equipped with a means to input the image data outputted from the digital camera 1, and the image data recorded with the digital camera 1 were changed, an image authentication system is constituted by the authentication program installed in the computer of personal computer 20 grade.

[0024] When formatted in the approach of connecting with the interface 17 of a digital camera 1 through serial cable 18 grade as a means to input image data and error detection data into a personal computer 20, and transmitting the JPEG file in a flash memory 16 to a personal computer 20, and the format which a flash memory 16 can detach and attach freely and is compatible with a personal computer 20, it is also possible to read directly the JPEG file 30 recorded on the flash memory 16 through the adapter with a personal computer 20.

[0025] When the encryption data 34 in the header unit 31 of the JPEG file 30 are enciphered with the private key within the digital camera 1, while an authentication program checks that it has been enciphered with the private key, it can decode a code by using a public key. It can judge whether image data is changed from the time of error detection data being generated by collating the decoded error detection data and image data. when the error detection data and the image data in which the encryption data 34 do not exist, which the encryption data 34 cannot decode with a public key and which were decoded were mismatching, the image data was not photoed with the digital camera 1 of this invention example -- it is regarded as what was changed after photography.

[0026] therefore, the photograph which printed the thing which recorded the file (this example JPEG file 30) containing the image data which the presenter of a photograph outputs from a digital camera 1, and is not adding modification when using the image authentication system of this invention example on record media, such as a floppy, or the thing which removed the flash memory 16 which is a removable record medium from the digital camera 1 -- a partner -- it responds for asking and submits. A reception side can check not having been changed since the time of the image data of the file being outputted

from a digital camera 1 by reading and investigating the file received using the authentication program installed in the personal computer 20.
[0027] Moreover, it can check that the image displayed as the printed photograph is the same by giving the function which displays the image of the image data of JPEG file 30 grade on an authentication program.
[0028] As mentioned above, as the example explained, it can check that it is the original thing by which the photograph taken with the digital camera is not changed from the time of photography and which is not altered by using the digital camera of this invention, and the image authentication system using it.
[0029] Although recorded on the image recording medium in the above-mentioned example by making into image data what carried out JPEG compression, this invention is applicable also to what was compressed by other compression approaches, and the thing which recorded non-compressed data as image data. Moreover, although error detection data were recorded on the header unit of a JPEG file, as this invention, error detection data may be in any location of image data. It is also possible not to be concerned with whether image data was compressed, lossless compression is carried out, or lossy compression is carried out, but to include the information on error detection data inside image data with the technique of an electronic watermark, so that it cannot distinguish with the naked eye.
[0030] Moreover, although error detection data and image data were recorded on one as a JPEG file in this example, error detection data may be recorded as another file, and you may relate with image data.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the flow chart which shows the procedure which records an image with the digital camera in the example of this invention.
[Drawing 2] It is the block diagram showing the digital camera by the example of this invention.
[Drawing 3] It is the mimetic diagram showing being used [CCD] for the digital camera by the example of this invention.
[Drawing 4] It is drawing for explaining how computing the checksum of the image data based on the example of this invention.
[Drawing 5] It is drawing for explaining the record approach of image data and error detection data by the example of this invention.
[Description of Notations]
1 Digital Camera
11 Control Unit
12 Condenser Lens
13 CCD (Photosensor)

14 A/D Converter
15 RAM
16 Flash Memory (Image Recording Medium)
17 Interface
18 Interconnection Cable
20 Personal Computer
30 JPEG File
31 Header Unit
32 Image Data
33 Checksum (Error Detection Data)
34 Encryption Data (Error Detection Data)

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－215452

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｎ　5/765		Ｈ０４Ｎ　5/781	５１０Ｆ
5/781			５１０Ｌ

審査請求　未請求　請求項の数４　ＯＬ　（全 ６ 頁）

(21)出願番号　特願平10－11408

(22)出願日　平成10年(1998)１月23日

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号

(72)発明者　中島　靖雅
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

(72)発明者　市原　信太郎
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

(72)発明者　最上　和人
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

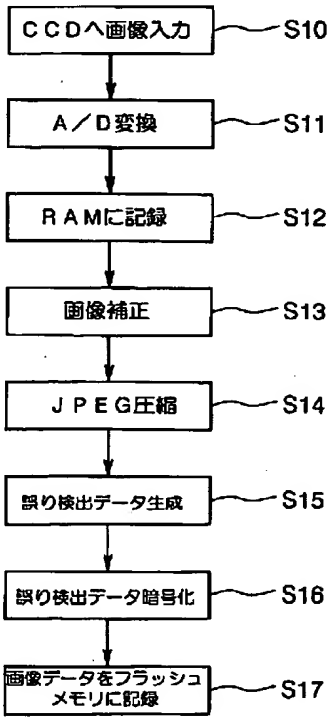
(74)代理人　弁理士　鈴木　喜三郎　（外２名）

(54)【発明の名称】　デジタルカメラおよびそれを用いた画像認証システム

(57)【要約】

【課題】　撮影時の画像データから変更されたか否かを確認することのできる画像データを出力するデジタルカメラを提供する。

【解決手段】　ステップＳ１１ではＣＣＤから出力された電気信号をデジタル信号に変換する。ステップＳ１２ではＡ／Ｄ変換器から出力されたデジタルデータをＲＡＭに記録する。ステップＳ１３ではＲＡＭに記録されたデータについて各種の画像補正を行う。ステップＳ１４ではステップＳ１３で補正されたデータをＪＰＥＧ方式により圧縮する。ステップＳ１５では圧縮された画像データから誤り検出データを生成する。ステップＳ１６では誤り検出データを暗号化して暗号化データとする。ステップＳ１７では画像データと暗号化データとを関連付けてＪＰＥＧファイルとしてフラッシュメモリに記録する。



1

【特許請求の範囲】

【請求項１】　複数の画素を有する光センサと、
前記光センサの出力をデジタル信号からなる画像データに変換する手段と、
前記画像データを記録する記録媒体と、
前記画像データから誤り検出データを生成する手段と、
前記画像データと前記誤り検出データとを関連付けて出力する手段と、を備えることを特徴とするデジタルカメラ。

【請求項２】　前記誤り検出データを暗号化する手段を備えることを特徴とする請求項１に記載のデジタルカメラ。

【請求項３】　前記記録媒体は着脱自在であり、前記画像データと前記誤り検出データとが関連付けて記録されることを特徴とする請求項１または２に記載のデジタルカメラ。

【請求項４】　請求項１～３のいずれか一項に記載のデジタルカメラを用いた画像認証システムであって、
画像データおよび誤り検出データを入力する手段と、
前記画像データを前記誤り検出データにより照合する手段と、を備えることを特徴とする画像認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、撮影した画像をデジタルデータとして記録するデジタルカメラに関するものである。

【０００２】

【従来の技術】従来より、写真を撮影するときには、レンズから取り込まれた光がフィルムの上に照射され、化学反応が起きることで画像が記録されるカメラが用いられている。上記のカメラでは、フィルムを現像し、印画紙に焼き付けることにより写真をプリントすることができる。上記の化学反応として一般に塩化銀の反応が利用されるため、このようなカメラによって撮影された写真を銀塩写真という。

【０００３】一方、近年ではＣＣＤ等の光センサにより光を電気信号に変換し、それをデジタル信号に変換してから、フラッシュメモリ等の記録媒体に記録するデジタルカメラが普及している。デジタルカメラを用いると、パソコン等を用いて画像の保存や様々な加工を個人で手軽に行えるほか、プリンタで出力することによりフィルムの現像をすることなしに写真を印刷することができる。プリンタの印刷品質の向上により、銀塩写真とほとんど区別がつかないほど品質の高い写真も印刷できるようになってきている。

【０００４】

【発明が解決しようとする課題】しかしながら、損害保険等の証明写真にデジタルカメラで撮影した写真を用いようとする場合に、デジタルカメラで撮影された画像はパソコン等により容易に加工が可能であり、銀塩写真と

2

比較して加工の跡を残さずに加工することができるため、不正に加工されたいわゆる改ざんされた写真が用いられていても判別することが困難であり、悪用される恐れがあるという問題がある。

【０００５】したがって、本発明の目的は撮影時の画像データから変更されたか否かを確認することのできる画像データを出力するデジタルカメラおよびそれを用いた画像認証システムを提供することにある。

【０００６】

【課題を解決するための手段】本発明の請求項１に記載のデジタルカメラによれば、画像データを記録する画像記録媒体と、画像データから誤り検出データを生成する手段と、画像データと誤り検出データとを関連付けて出力する手段とを備える。従って、撮影時に記録媒体に記録された画像データが、デジタルカメラから出力後に１ビットでも変更された場合には、画像データと誤り検出データとが不整合となるため、撮影後に画像データが変更されたと判断することができる。また、画像データと誤り検出データとの整合性がとれていれば、画像は撮影時のままであると判断することができる。誤り検出データを生成する方法としては、画像データのチェックサムを求める方法や、ＣＲＣ（Cyclic Redundancy check）あるいは一方向ハッシュ関数（one-way hash function）などを用いることができる。

【０００７】本発明の請求項２に記載のデジタルカメラによれば、誤り検出データは暗号化されるため、画像データが同一の誤り検出データを得られる別の画像データに変更されることや、画像データの変更に合わせて誤り検出データが書き換えられるのを防ぐことができる。

【０００８】本発明の請求項３に記載のデジタルカメラによれば、画像記録媒体は着脱自在であるため、画像記録媒体をデジタルカメラからの出力手段として用いることができる。また、デジタルカメラから取り外した画像記録媒体をパソコン等により直接読取って画像データを入力する場合に、撮影時から変更されたか否かを判断可能な画像データとして出力するためには、画像データと誤り検出データとが画像記録媒体に関連付けて記録されることが必要である。

【０００９】本発明の請求項４に記載の画像認証システムによれば、画像データおよび誤り検出データを入力する手段と、画像データを誤り検出データにより照合する手段とを備えるため、入力された画像データがデジタルカメラによって記録されてから変更されたか否かを判断することができる。

【００１０】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【００１１】図２は本発明の実施例のデジタルカメラ１を説明するためのブロック図である。制御装置１１、集光レンズ１２、光センサとしてのＣＣＤ（Charge Coupl

edDevice）１３、Ａ／Ｄ変換器１４、ＲＡＭ（Random Access Memory）１５、画像データを記録する画像記録媒体としてのフラッシュメモリ１６、フラッシュメモリ１６の内容を外部のパソコン２０等に出力するためのインターフェイス１７などから構成される。制御装置１１はＣＰＵと、デジタルカメラ１の様々な制御を行うためのプログラムが記録されたＲＯＭと、入出力手段とを備える。

【００１２】図１はデジタルカメラ１により撮影が行われる行程を示すフローチャートである。ユーザーがデジタルカメラ１のシャッターを押すと、ステップＳ１０で、集光レンズ１２により集光された光がＣＣＤ１３に入力され、電気信号に変換される。集光レンズ１２の絞りやシャッタースピード、すなわちＣＣＤ１３の蓄積時間は制御装置１１によって自動的に、またはユーザーの指示によって制御される。ＣＣＤ１３として、例えば図３に示すようにＲ（Red）、Ｇ（Green）、Ｂ（Blue）の原色フィルタを有する複数の画素がマトリックス状に配置されたＣＣＤ１３を用いることにより、カラー画像を撮影することができる。Ｃ（Cyan）、Ｍ（Magenta）、Ｙ（Yellow）、Ｇ（Green）の補色フィルタを有するＣＣＤを用いる場合もある。

【００１３】ステップＳ１１では、ＣＣＤ１３から出力された電気信号がＡ／Ｄ変換器１４によりデジタル信号に変換され、ステップＳ１２ではＡ／Ｄ変換器１４から出力されたデジタルデータが高速化のためＤＭＡ（Direct Memory Access）により制御装置１１を介さずに直接ＲＡＭ１５のアドレスを指定して記録される。ＲＡＭ１５としてはセルフリフレッシュ機能をもつＤＲＡＭを用いることができる。

【００１４】ステップＳ１３では、ＲＡＭ１５に記録されたデータについて、ホワイトバランスの調整、補間処理、色補正などの各種の画像補正が行われる。

【００１５】ステップＳ１４では、画像記録媒体への記録枚数を多くするためにステップＳ１３で補正されたデータをＪＰＥＧ（Joint Photographic Experts Group）などの方式により圧縮し、容量の小さな画像データを生成する。ＪＰＥＧはＲ、Ｇ、Ｂの各色２５６階調の約１６７０万色の画像を扱うことができ、一般に用いられる不可逆画像圧縮方法であり、圧縮率を変更することにより保存画質を調整することができる。ＪＰＥＧ圧縮は、制御装置１１によってソフトウェア的に行うほか、高速化のために専用の回路を用いることができる。

【００１６】ステップＳ１５では、ステップＳ１４で生成された画像データに基づいて、制御装置１１により誤り検出データを生成する。誤り検出データとしては、例えばチェックサムを用いることができる。ここで、画像データ３２を２進数で表したものが、図４のように示されるとする。図４のＡに示すように、画像データの横方向の８ビットの桁上げなしの合計値を制御装置１１によ

りそれぞれの行で計算し、それをチェックサム３３とすると、画像データ３２が変更された場合には、画像データ３２から求められる合計値とチェックサム３３が不整合となるので、画像データ３２とチェックサム３３とを照合することにより画像データ３２が変更されたか否かを判断することができる。この場合、１行の中で２ビットが変更されると、変更されたことを検出することができないため、図４のＢに示すように縦方向の８ビットについてもそれぞれの列で合計値を計算したチェックサム３３をさらに用いてもよい。

【００１７】また、チェックサムの他にＣＲＣ方式、一方向ハッシュ関数等、データがオリジナルから変更されているか否かを検出することができる、データ通信等に用いられる誤り検出に関する公知の方法を本発明に適用することができる。これらの方法を用いることにより、各々の画像データに対して異なる誤り検出データを割り当てることができ、また、誤り検出データから元の画像データを再現することは非常に困難であり、実用上の問題は無いといえる。

【００１８】ステップＳ１６では、チェックサム３３等の誤り検出データが解析されたり容易に書き換えられたりしないように、制御装置１１により暗号化して暗号化データ３４とする。暗号化の方法としては、公開鍵と秘密鍵を用いるＲＡＳ方式など、公知の方法を用いることができる。秘密鍵で暗号化した暗号化データ３４は、秘密鍵と対になった公開鍵を用いて解読することができる。秘密鍵はデジタルカメラ１内に記憶されており、他人に知られてはならない。また、ユーザーが秘密鍵を知らなくてもよい。しかし、公開鍵から秘密鍵を求めることは非常に困難である。これにより、画像データ３２が同一のチェックサム３３を得られる別の画像データに変更されることや、画像データ３２の変更に合わせてチェックサム３３が書き換えられるのを防ぐことができる。

【００１９】ステップＳ１７では、画像データ３２と暗号化データ３４とを一体にＪＰＥＧファイル３０として画像記録媒体としてのフラッシュメモリ１６に記録する。フラッシュメモリ１６は通電し続けなくても一旦記録した内容を保持することのできる書換え可能な記録媒体であり、デジタルカメラ１に内蔵されるか、あるいは着脱自在にデジタルカメラ１に取り付けられている。ＪＰＥＧファイル３０は一般に図５に示すようにデータ長、圧縮率等の情報を含むヘッダ部３１と、画像データ３２とから構成される。デジタルカメラ１によって記録されるＪＰＥＧファイル３０の場合は、撮影日やシャッタースピード等の撮影条件等の情報もヘッダ部３１に記録することができる。本実施例では、ヘッダ部３１に暗号化データ３４を更に加えて記録している。

【００２０】フラッシュメモリ１６がデジタルカメラ１に内蔵されていて、取り外しが不可能な場合には、フラッシュメモリ１６には暗号化データ３４等の誤り検出デ

ータを含まないＪＰＥＧファイル３０を記録しておき、インターフェイス１７を介して外部のパソコン２０に出力する段階で誤り検出データを生成し、ＪＰＥＧファイル３０のヘッダ部３１に付加して出力することも可能である。なお、パソコン２０からデジタルカメラ１に画像を転送できるようになっている場合は、ＪＰＥＧファイル３０のヘッダ部３１等により区別して、再度パソコン２０に転送するときには誤り検出データを付加しないようにする必要がある。

【００２１】一方、フラッシュメモリ１６がデジタルカメラ１から着脱自在で、その内容をパソコン等によって読み取り可能な場合、あるいはデジタルカメラ１自体に画像を修正する機能が備えられている場合には、画像データと誤り検出データとを一体に出力するためには画像データがフラッシュメモリ１６に記録される段階で、同時に誤り検出データが記録されている必要がある。

【００２２】また、図１に示す本実施例のフローチャートでは、ステップＳ１３の次にステップＳ１４で画像データをＪＰＥＧ圧縮し、その後にステップＳ１５、Ｓ１６を実行し、誤り検出データの生成と暗号化を行ったが、ステップＳ１３の次にステップＳ１５、Ｓ１６を実行し、そのあとにステップＳ１４で画像データをＪＰＥＧ圧縮することも可能である。

【００２３】上記のようなデジタルカメラ１と、デジタルカメラ１から出力された画像データを入力する手段を備えるパソコン２０と、デジタルカメラ１によって記録された画像データが変更されたか否かを判定するためにパソコン２０等のコンピュータにインストールされた認証プログラムとによって画像認証システムが構成される。

【００２４】パソコン２０に画像データと誤り検出データを入力する手段としては、シリアルケーブル１８等を介してデジタルカメラ１のインターフェイス１７と接続してフラッシュメモリ１６内のＪＰＥＧファイルをパソコン２０に転送する方法や、フラッシュメモリ１６が着脱自在でパソコン２０と互換性のある形式でフォーマットされている場合には、アダプタを介してフラッシュメモリ１６に記録されたＪＰＥＧファイル３０をパソコン２０で直接読み取ることも可能である。

【００２５】ＪＰＥＧファイル３０のヘッダ部３１内の暗号化データ３４がデジタルカメラ１内で秘密鍵によって暗号化されている場合、認証プログラムは公開鍵を用いることにより、秘密鍵によって暗号化されたことを確認すると同時に暗号を解読することができる。解読された誤り検出データと、画像データとを照合することによって、誤り検出データが生成された時点から画像データが変更されているか否かを判断することができる。暗号化データ３４が存在しない、暗号化データ３４が公開鍵で解読できない、解読された誤り検出データと画像データとが不整合である場合には、その画像データは本発明

実施例のデジタルカメラ１で撮影されたものではないか、撮影後に変更されたものとみなされる。

【００２６】したがって、本発明実施例の画像認証システムを使用する場合、写真の提出者は、デジタルカメラ１から出力して変更を加えていない画像データを含むファイル（本実施例ではＪＰＥＧファイル３０）をフロッピー等の記録媒体に記録したもの、あるいは着脱可能な記録媒体であるフラッシュメモリ１６をデジタルカメラ１から取り外したものを、印刷した写真と共に相手の求めに応じて提出する。受け取り側は、パソコン２０にインストールされた認証プログラムを用いて受け取ったファイルを読み込んで調べることにより、そのファイルの画像データがデジタルカメラ１から出力された時点から変更されていないということを確認することができる。

【００２７】また、認証プログラムにＪＰＥＧファイル３０等の画像データの画像を表示する機能をもたせることにより、印刷された写真と表示された画像が同一であることを確認することができる。

【００２８】以上、実施例によって説明したように、本発明のデジタルカメラおよびそれを用いた画像認証システムを用いることにより、デジタルカメラで撮影した写真が撮影時から変更されていない、改ざんされていない、オリジナルのものであることを確認することができる。

【００２９】上記の実施例では、ＪＰＥＧ圧縮したものを画像データとして画像記録媒体に記録したが、本発明は他の圧縮方法で圧縮したものや、無圧縮のデータを画像データとして記録したものにも適用できる。また、誤り検出データをＪＰＥＧファイルのヘッダ部に記録したが、本発明としては誤り検出データは画像データのどの位置にあってもよい。画像データが無圧縮であるか、可逆圧縮されたものであるか、あるいは不可逆圧縮されたものであるかに関わらず、電子すかしの技術により、肉眼では判別できないように誤り検出データの情報を画像データの内部に含ませることも可能である。

【００３０】また、本実施例では誤り検出データと画像データとを一体にＪＰＥＧファイルとして記録したが、誤り検出データを別ファイルとして記録し、画像データに関連付けてもよい。

【図面の簡単な説明】

【図１】本発明の実施例におけるデジタルカメラにより画像を記録する手順を示すフローチャートである。

【図２】本発明の実施例によるデジタルカメラを示すブロック図である。

【図３】本発明の実施例によるデジタルカメラに用いられるのＣＣＤを示す模式図である。

【図４】本発明の実施例による画像データのチェックサムを算出する方法を説明するための図である。

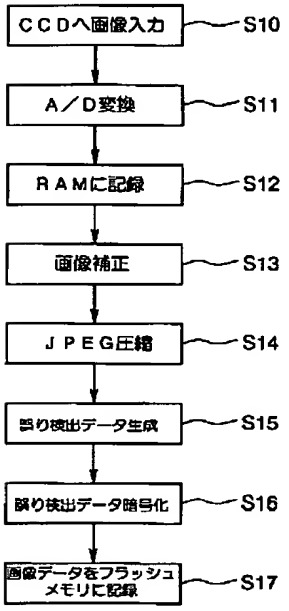
【図５】本発明の実施例による画像データと誤り検出データの記録方法を説明するための図である。

【符号の説明】

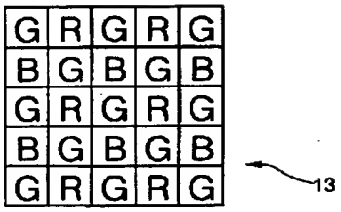
1　デジタルカメラ
11　制御装置
12　集光レンズ
13　ＣＣＤ（光センサ）
14　Ａ／Ｄ変換器
15　ＲＡＭ
16　フラッシュメモリ（画像記録媒体）

17　インターフェイス
18　接続ケーブル
20　パソコン
30　ＪＰＥＧファイル
31　ヘッダ部
32　画像データ
33　チェックサム（誤り検出データ）
34　暗号化データ（誤り検出データ）

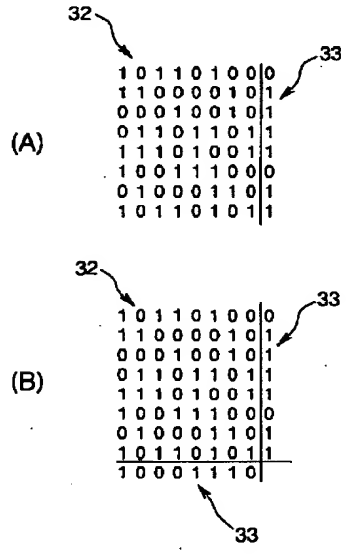
【図１】



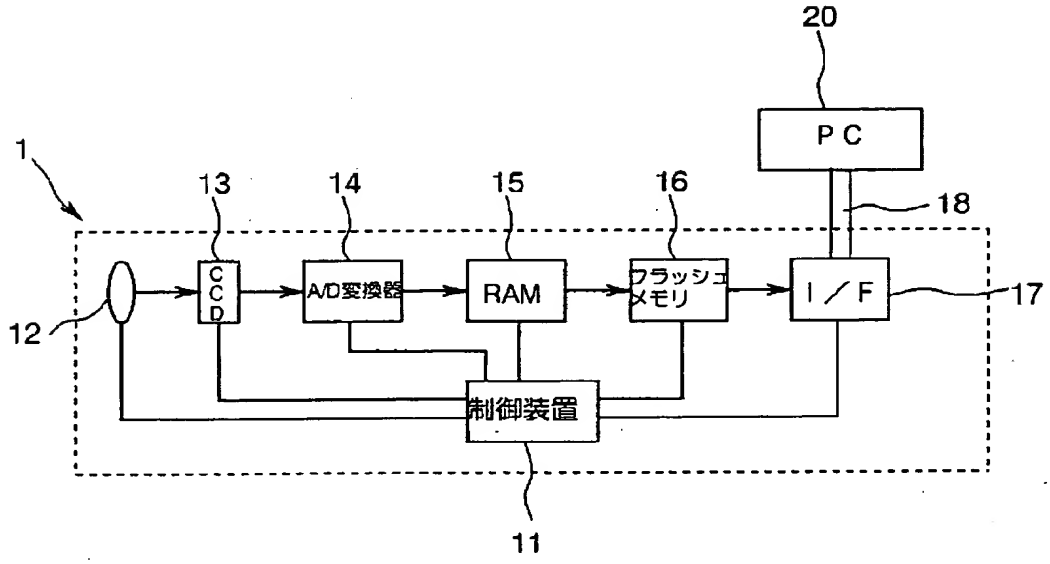
【図３】



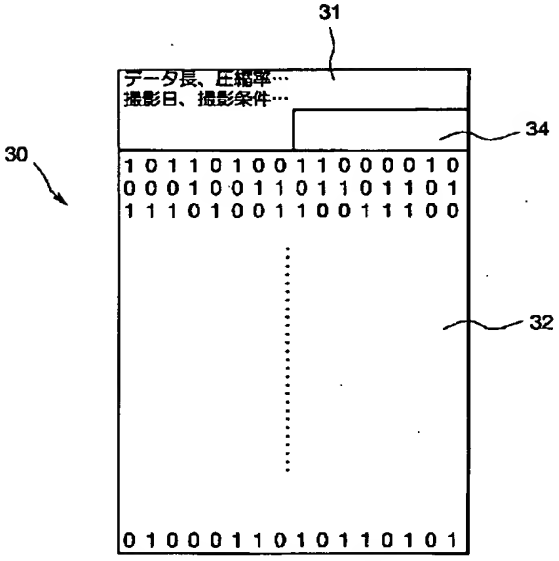
【図４】



【図２】



【図５】


31
データ長、圧縮率…
撮影日、撮影条件…
34
30
1 0 1 1 0 1 0 0 1 1 0 0 0 0 1 0
0 0 0 1 0 0 1 1 0 1 1 0 1 1 0 1
1 1 1 0 1 0 0 1 1 0 0 1 1 1 0 0
32
0 1 0 0 0 1 1 0 1 0 1 1 0 1 0 1